REMARKS

I. Introduction

In response to the Office Action dated August 21, 2008, the claims have not been amended. Claims 1-48 remain in the application. Re-examination and re-consideration of the application is requested.

II. Summary of the Invention

The independent claims are generally directed to distributing content throughout a household network using a host IRD that receives the broadcast content via satellite and relays it for display by trusted light weight client boxes. More specifically, in claims 1 and 7, the claims provide for receiving and decrypting an encrypted media encryption key at a host receiver. The decrypted key is then re-encrypted by the host receiver using a pairing key. The re-encrypted key is transmitted from the host to the client. The claims specifically recite that the client does not utilize a conditional access module (CAM). Thus, the client receiver is a light-weight box. Thereafter, the client decrypts the key using the pairing key. The host then receives encrypted program material (that has been broadcast) and transfers the material to the client receiver. The client receiver decrypts the encrypted program materials using the decrypted media encryption key.

Similar to claims 1 and 7, claims 13 and 22 claim very similar limitations but further provide for the host receiver to use a conditional access module (CAM). In this regard, the first portion of claims 13 and 22 provide for the synchronization between the CAM and the host. The second part transmits the materials and keys to the client.

Similar to claims 1, 7, 13, and 22, claims 31 and 38 first synchronize the CAM on the host with the client receiver and then send program materials from the host to the client.

One unique aspect about all of the claims is that the client is a light-weight client and does not utilize a CAM. Further, as recited in the amended dependent claims 43-48, the light-weight client also lacks a tuner and explicitly provides that the host utilizes a CAM.

The chart below indicates support in the specification for the claims.

CLAIM LIMITATION	SPECIFICATION/DRAWING SUPPORT
1. A method of distributing	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B

program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:	
(a) receiving an encrypted media encryption key at the host receiver;	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-P16,L3; P17,L4-9; FIG. 7B-732;
(b) decrypting the encrypted media encryption key at the host receiver;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key;	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) transferring the re-encrypted media encryption key from the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(f) receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;
(g) transferring the encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.
7. An apparatus for distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B
(a) means for receiving an encrypted	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-

media encryption key at the host receiver;	P16,L3; P17,L4-9; FIG. 7B-732;
(b) means for decrypting the encrypted media encryption key at the host receiver;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) means for re-encrypting the decrypted media encryption key at the host receiver using a pairing key;	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) means for transferring the re-encrypted media encryption key from the host receiver to the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(e) means for decrypting the re-encrypted media encryption key at the client receiver using the pairing key;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(f) means for receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;
(g) means for transferring the encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(h) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.
13. A method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B
(a) receiving an encrypted media encryption key at a conditional access module associated with the host receiver;	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-P16,L3; P17,L4-9; FIG. 7B-732;

(b) decrypting the encrypted media encryption key at the conditional access module;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) re-encrypting the decrypted media encryption key at the conditional access module using a first pairing key shared between the conditional access module and the host receiver;	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) transferring the re-encrypted media encryption key from the conditional access module to the host receiver;	P6,L3-16; P17,L14-20; FIG. 7B-402,124;
(e) receiving the re-encrypted media encryption key at the host receiver from the conditional access module;	P6,L3-16; P17,L14-20; FIG. 7B-402,124;
(f) decrypting the re-encrypted media encryption key at the host receiver using the first pairing key shared between the conditional access module and host receiver;	P6,L3-16; P17,L14-20; FIG. 7B-402,124;
(g) re-encrypting the decrypted media encryption key at the host receiver using a second pairing key shared between the host receiver and the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P6,L3-16; P17,L21-25; FIG. 7B-748,124,402,750;
(h) transferring the re-encrypted media encryption key from the host receiver to the client receiver; and	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(i) decrypting the re-encrypted media encryption key at the client receiver using the second pairing key shared between the host receiver and the client receiver;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(j) receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;

(k) transferring encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(l) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.
22. An apparatus for distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B
(a) means for receiving an encrypted media encryption key at a conditional access module associated with the host receiver;	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-P16,L3; P17,L4-9; FIG. 7B-732;
(b) means for decrypting the encrypted media encryption key at the conditional access module;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) means for re-encrypting the decrypted media encryption key at the conditional access module using a first pairing key shared between the conditional access module and the host receiver;	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) means for transferring the re-encrypted media encryption key from the conditional access module to the host receiver;	P6,L3-16; P17,L14-20; FIG. 7B-402,124;
(e) means for receiving the re-encrypted media encryption key at the host receiver from the conditional access module;	P6,L3-16; P17,L14-20; FIG. 7B-402,124;
(f) means for decrypting the re-encrypted media encryption key at the host receiver using the first pairing key shared between the	P6,L3-16; P17,L14-20; FIG. 7B-402,124;

conditional access module and host receiver;	
(g) means for re-encrypting the decrypted media encryption key at the host receiver using a second pairing key shared between the host receiver and the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P6,L3-16; P17,L21-25; FIG. 7B-748,124,402,750;
(h) means for transferring the re-encrypted media encryption key from the host receiver to the client receiver; and	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(i) means for decrypting the re-encrypted media encryption key at the client receiver using the second pairing key shared between the host receiver and the client receiver;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(j) means for receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;
(k) means for transferring encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(l) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.
31. A method of distributing program materials received from a broadcast system between a host and client receiver for remote decryption, comprising:	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B
(a) receiving an encrypted media encryption key at a conditional access module associated with the host receiver;	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-P16,L3; P17,L4-9; FIG. 7B-732;

(b) decrypting the encrypted media encryption key at the conditional access module;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) re-encrypting the decrypted media encryption key at the conditional access module using a pairing key shared between the conditional access module and the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) transferring the re-encrypted media encryption key from the conditional access module to the client receiver;	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key shared between the conditional access module and client receiver;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(f) receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;
(g) transferring encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.
38. An apparatus for distributing program materials received from a broadcast system between a host and client receiver for remote decryption, comprising:	P4, L11-12; P5,L15-17; P12,L10-11; FIG. 7A-7B
(a) means for receiving an encrypted media encryption key at a conditional access module associated with the host receiver;	P6,L10-11; P15,L19-24; FIG. 7A-702; P15,L28-P16,L3; P17,L4-9; FIG. 7B-732;

(b) means for decrypting the encrypted media encryption key at the conditional access module;	P6,L10-16; P15,L19-24; FIG. 7A-702, 402, 704; P17,L4-9; FIG. 7B-732-402,414,734;
(c) means for re-encrypting the decrypted media encryption key at the conditional access module using a pairing key shared between the conditional access module and the client receiver, wherein the client receiver does not utilize a conditional access module (CAM);	P15,L25-27; FIG. 7-706,708; P17,L10-13; FIG. 7B-736,124,738; P17,L21-25; FIG. 7B-124,748,402,750;
(d) means for transferring the re-encrypted media encryption key from the conditional access module to the client receiver;	P5,L18-21; L26-29; P6,L10-16; P16,L4-7; FIG. 7-718,124; P17,L26-30; FIG. 7B-124,752,754,756.
(e) means for decrypting the re-encrypted media encryption key at the client receiver using the pairing key shared between the conditional access module and client receiver;	P5,L27-29; P6,L10-16; P12,L6-22; P13,L22-P14,L4; FIG. 6; P15,L28-P16,L3; P17,L14-20; P18,L1-7; FIG. 7B-754; FIG. 5-124,414;
(f) means for receiving encrypted program materials from the broadcast system at the host receiver;	P5,L18-21; P15,L19-24; P16,L12-18; FIG. 7A-700; P17,L4-9; FIG. 7B-730;
(g) means for transferring encrypted program materials from the host receiver to the client receiver; and	P16,L4-7; FIG. 7A-124; P16,L12-18; FIG. 7A-726,728; P18,L1-12; FIG. 7B-762
(h) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.	P16,L12-18; FIG. 7A-726,124; P18,L1-12; FIG. 7B-762,124.

III. Prior Art Rejections

On pages (6)-(13) of the Office Action, claims 1-12, 45 and 46 were rejected under 35 U.S.C. §103(a) as being obvious in view of the combination of Raike et al., U.S. Publication 2002/0162104 (Raike), Son et al., U.S. Publication 2001/0017920 (Son) and Akiyama, U.S. Publication 2002/0001386 (Akiyama).

On page (13) of the Office Action, claims 47 and 48 were rejected under 35 U.S.C. §103(a) as being obvious in view of the combination of Raikie, Son, Akiyama and Loisel, U.S. Publication 2003/0026428 (Loisel).

On pages (14)-(22) of the Office Action, claims 13-44 were rejected under 35 U.S.C. §103(a) as being obvious in view of the combination of Raike, Loisel, Son and Akiyama.

The rejections of the claims were identical to that of the prior rejections. Accordingly, Applicants reassert that previously asserted arguments as set forth below.

Applicant respectfully disagrees with and traverses the above rejections for at least one or more of the following reasons:

(1) Neither Raike, Son, Akiyama, nor Loisel teach, disclose, or suggest a single host receiver that is configured to perform multiple specifically claimed activities including decrypting and re-encrypting a media encryption key, transferring a re-encrypted media key to a client, receiving encrypted program materials that have been broadcast, and transferring received broadcast materials to a client;

(2) Neither Raike, Son, Akiyama, nor Loisel teach, disclose, or suggest a client receiver that does not have a CAM that is configured to perform multiple specifically claimed limitations including decrypting a re-encrypted media encryption key and decrypting received program materials using the decrypted media encryption key; and

(3) Raike teaches away from the presently claimed invention.

The independent claims are generally directed to distributing content throughout a household network using a host IRD that receives the broadcast content via satellite and relays it for display by trusted light weight client boxes. More specifically, in claims 1 and 7, the claims provide for receiving and decrypting an encrypted media encryption key at a host receiver. The decrypted key is then re-encrypted by the host receiver using a pairing key. The re-encrypted key is transmitted from the host to the client. The claims specifically recite that the client does not utilize a conditional access module (CAM). Thus, the client receiver is a light-weight box. Thereafter, the client decrypts the key using the pairing key. The host then receives encrypted program material (that has been broadcast) and transfers the material to the client receiver. The client receiver decrypts the encrypted program materials using the decrypted media encryption key.

Similar to claims 1 and 7, claims 13 and 22 claim very similar limitations but further provide for the host receiver to use a conditional access module (CAM). In this regard, the first portion of

claims 13 and 22 provide for the synchronization between the CAM and the host. The second part transmits the materials and keys to the client.

Similar to claims 1, 7, 13, and 22, claims 31 and 38 first synchronize the CAM on the host with the client receiver and then send program materials from the host to the client.

One unique aspect about all of the claims is that the client is a light-weight client and does not utilize a CAM. Further, as recited in the amended dependent claims 43-48, the light-weight client also lacks a tuner and explicitly provides that the host utilizes a CAM.

In rejecting claims 1 and 7, the Office Action primarily relies on Raike. Specifically, the Action equates the claimed client receiver to Raike's consumers or end-users through the use of client devices. The Action further equates the claimed host receiver to Raike's retail server. For such a rejection to establish a prima facie case of nonobviousness, Raike's client devices and retail server must perform the functionalities of the client device and host receiver respectively. Thus, Raike's retail server must be able to receive an encrypted media encryption key, decrypt the media encryption key, re-encrypt the decrypted media encryption key and forward/transfer the re-encrypted key to the client receiver. In addition, Raike's retail server must also receive encrypted program materials and transfer it to a client receiver.

However, contrary to that set forth in the Office Action, Raike completely and entirely fails to disclose such capabilities. Instead, Raike actually teaches away from having a single retail server perform such multiple functions. In fact, multiple different paragraphs of Raike explicitly teach away from such a single retail server performing the multiple functions. Applicants direct the attention of the Patent Office to paragraph [0037] which provides:

> ...It is part of the invention that the encrypted content is made available separately from the encryption keys or access rights and these rights or keys are purchased or otherwised acquired by consumers from an entity who holds neither media or keys. Additionally security is maximised if all three functions are managed by separate entities from separate server sites.

Similarly, paragraph [0039] provides:

> ...To best secure the media it is important for the key server and media server to be managed by separate entities.

Thus, as can be clearly seen, Raike explicitly and expressly provides for using multiple different servers and requires that the key server be separate from the media server. Further, Raike explicitly requires that the key functionality is managed by separate entities from separate server sites. Such a teaching serves to explicitly teach away from the presently claimed invention which

expressly requires that the host receiver perform both functions. Thus, Raike should not and cannot be used to reject the portions of the claim upon which it is relied for.

The Action acknowledges Raike's lack of disclosure with respect to the decryption and re-encryption of the media encryption key (see Page 3 of the Action). However, as described above, in addition to failing to teach such elements, Raike actually teaches away from a single server that both receives the media AND performs encryption services relating to the media encryption key.

The Action ignores this combined functionality of the claimed host receiver and combines multiple different references. Again, since Raike teaches away from such functionality, even combining Raike with another reference would still fail to render the claimed invention obvious.

To teach the decrypting/re-encrypting functionality of the claimed host receiver, the Office Action relies on Son. Applicants note that Son fails to teach, describe, or suggest, explicitly or implicitly, the use of a light-weight client receiver. More specifically, Son does not hint at or remotely allude to the use of a client box that does not have nor utilize a conditional access module (CAM). Instead, Son is directed towards video-on-demand distribution networks (see paragraph [0007]) and a standard distribution network which is commonly known to include and utilize conditional access modules (CAMs).

In rejecting these claim elements, the Action asserts that since Son discloses decrypting and re-encrypting a video program, it teaches the decrypting and re-encrypting of a key since any data can be decrypted and re-encrypted. Applicants respectfully disagree with and traverse such an assertion. In this regard, the claims explicitly provide for a process that utilizes specific keys for specific functions. Further, the claims provide for decrypting and re-encrypting a media key that is then used to decrypt actual media content. To assert that the media content is equivalent to such a key is wholly without merit and illogical. Further, contrary to that asserted in the Action, one of ordinary skill in the art would not compare a program that is being encrypted to encrypting a key that is used to decrypt such a program. Again, it is not only illogical but disingenuous to make such an assertion.

Lastly, the Action acknowledges that Raike and Son both fail to disclose the use of a pairing key for content between a host receiver and a client receiver. Instead, the Action relies on Akiyama (paragraphs [0099] and [0100]) for such a teaching. Applicants note that paragraph [0099] recites that each receiver apparatus has a master key which is used to encrypt a channel key. Also of note is that Akiyama's receiver apparatus is within the prior art devices in that they all receive direct broadcasts and therefore include a broadcast wave receiver 111 (see FIG. 1) and include IC cards

(e.g., see paragraphs [0154] and [0262]). Thus, rather than teaching a thin client box or a client receiver box that does not have a CAM yet also has a pairing key to a host receiver, Akiyama merely discloses receiver boxes that receive broadcasts without any host receiver whatsoever. The Action equates Akiyama's broadcast center to the claimed host. However, as can be clearly seen in the claims, the claimed host receives media that is broadcast and forwards/transfers it to the client device. Thus, the host does not have the broadcast functionality or capabilities as is required in Akiyama.

Again, the present invention is unique in that it relates to a thin client box configuration with a host that receives broadcasts and transmits them to one or more client thin boxes. In addition, the media keys necessary to view the programs that were broadcast are managed by the host receiver and encrypted and sent to the thin client boxes. Such capabilities are neither taught nor suggested in any way, shape, or form, explicitly or implicitly, by any of the cited references, either alone or in combination.

Further, the dependent claims more clearly establish that the client receiver does not and cannot receive broadcasts because it does not have a tuner. Further, while the client device does not have a tuner, the host receiver has a conditional access module that is used to receive and manage the programs that the host receives via broadcast.

In addition to the above, Loisel fails to cure the deficiencies of the other cited references. In this regard, the Action relies on Loisel to teach a host receiver using a CAM. However, similar to the limitations of the other cited references, Loisel does not even contemplate a thin client box and host receiver configuration as set forth in the present claims. In this regard, Loisel fails to disclose a client box that does not have a tuner configured/paired with a host receiver that utilizes a CAM as claimed. Instead, Loisel discloses the use of a smart card which is similar to a CAM as well as a CAM.

In response to the above arguments, the Office Action equates the claimed client devices to Raike's set-top boxes and the claimed host receiver to Raike's retail server based on paragraph [0038]. Applicants respectfully disagree with such an assertion. Namely, the claims explicitly recite that the claimed client device does NOT utilize a CAM. The standard set-top box including that of Raike include CAMs. Thus, there is no possible way for Raike's client device to be equivalent to the claimed client receiver. In rejecting the claim element relating to the lack of a CAM, the Office Action relies on paragraph Raike [0017] which consists of one sentence "downloading said

encrypted media key to said client device". The assertion that such a sentence discloses the lack of a CAM within the receiving device is wholly improper and lacks any foundation whatsoever.

The Action later continues and provides that Son discloses receiving encrypted data at the host receiver and that a store, decrypt and re-encrypt process may be performed on any media data. Again, the Examiner is relying on impermissible hindsight offered only after reading the disclosure of the present invention. Further, the Examiner is relying on his/her own knowledge without taking official notice and without support in the cited references. Again, the present claims provide for a the use of thin client devices without CAMs and provide for a specific system and method for encrypting and using keys and program materials – all of which are lacking as described above. Further, it is well known that in a video distribution system such as that described in Son, a CAM exists in the client receiver. Accordingly, the devices described in Son are not thin client devices without CAMs as required in the claims. To date, the Examiner has failed to provide any evidence or even a remote inference that any of the client based boxes do not have CAMs. Accordingly, the rejections are in error and fail to establish a prima face case of unpatentability.

The Office Action further acknowledges Raike and Son's failure to use a pairing key for content between a host and client. Instead, the Action relies on Akiyama. As stated above, Akiyama clearly and explicitly requires the use of a CAM and therefore fails to meet the same claim limitations that the other references do. Further, such an explicit use of an IC card would serve to teach away from the present invention. Again, the present claims address the use of a thin client receiver that does not have a CAM – none of the cited references teach such a thin client whatsoever, explicitly or implicitly.

Applicants previously asserted arguments with respect to claims 45-46 in that none of the cited references teach that a client receiver does not have a tuner. The pending Office Action asserts that Raike teaches the lack of a tuner in paragraph [0038] since set-top boxes are not tuners. Applicants respectfully disagree with and traverse such an assertion. It is well known that set-top boxes customarily include tuners in order to tune the particular media content being received. Without such tuners, the standard set top boxes would not be very useful. The present claims provide an advantage by using a thin client system without a tuner. The Examiner asserts that set-top boxes are not tuners without any foundation or support in the cited references and in a manner that is inconsistent with standard set-top boxes that are also referred to as tuner/demodulator boxes and require and utilize tuners. Again, the present claims address a unique situation where not only

does the client receiver not have a tuner or a CAM, but the host receiver utilizes a CAM instead. Such an architecture is wholly and completely lacking from the cited art.

The Office Action further proceeds to rely on Loisel for a host receiver utilizing a CAM. While Loisel discloses a CAM used in a second communication device, the architecture established in the claims with a client receiver not utilizing a CAM and decrypting content received from the host receiver is nowhere to be found in Loisel.

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over Raike, Son, Akiyama, and Loisel. In addition, Applicants' invention solves problems not recognized by Raike, Son, Akiyama, and Loisel. In this regard, while the present invention is directed towards the use of lightweight client boxes in a home network, neither Raike, Son, Akiyama, nor Loisel even recognize the use or possible use of a home network or any problems associated with such a network.

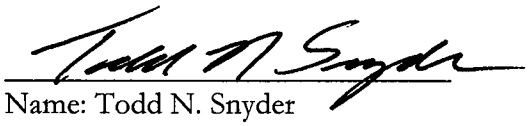
Thus, Applicants submit that the independent claims are allowable over Raike, Son, Akiyama, and Loisel. Further, the dependent claims are submitted to be allowable over Raike, Son, Akiyama, and Loisel in the same manner, because they are dependent on the independent claims, and thus contain all the limitations of the independent claims. In addition, the dependent claims recite additional novel elements not shown by Raike, Son, Akiyama, and Loisel.

IV. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Should any fees be associated with this submission, please charge Deposit Account 50-0383.

Respectfully submitted,



Date: November 20, 2008

Name: Todd N. Snyder
Reg. No.: 41,320

The DIRECTV Group, Inc.
CA/LA1/A109
2230 E. Imperial Highway
El Segundo CA 90245

Telephone No. (310) 964-0560